Email Hygiene and Encryption Standard

EA Technology Standard TRM 2.8.861.001

Status: Pending Approval
Analysis: (Burton Group, Microsoft, Best Practices, Office of Technology Services (OTech))
Effective Date: Nov 5, 2009
Next Review Date: Nov 5, 2010
Approved By: Office of the Chief Information Officer (OCIO)

Introduction
The purpose of this Email Hygiene and Encryption Standard (E-Hub) is to define the centralized email hygiene and encryption service standard to be used by all email systems within the Executive Branch of state Government. All other statewide offices may choose to use the E-Hub service. The Email hygiene solution is a comprehensive tool/service that includes anti-spam filtering, anti-virus scanning of email messages and attachments, email content/policy filtering, and email encryption. This service will enhance the security and protection of statewide email services and diminish the impact of spam on the state's networks. In addition, the centralized E-Hub solution will reduce the use of disparate email hygiene tools which will further the intent of Government Code 11545(b) (3) which is to minimize overlap, redundancy and cost in state operations by promoting the efficient and effective use of Information Technology (IT).

Standard
Centralized email filtering and encryption is delivered through the OTech E-Hub service. The E-Hub service provides email filtering, anti-virus, malware and encryption through the following cloud based services from Microsoft:

- Microsoft Forefront Online Protection for Exchange
  - Forefront Online Protection for Exchange consists of layered technologies to actively help protect businesses' inbound and outbound e-mail from spam, viruses, phishing scams, and e-mail policy violations.

- Microsoft Exchange Hosted Encryption
  - Microsoft Exchange Hosted Encryption provides policy-based encryption from sender to recipient with no end-user training or software installation.

Authorities
Governor's Reorganization Plan Statutory Provision SEC. 17. Section 11545 of the Government (b) The duties of the State Chief Information Officer shall include, but are not limited to, all of the following: (2) Establishing and enforcing state information technology strategic plans, polices, standards, and enterprise architecture.

Implementation:
To transition to E-Hub, agencies must submit a standard Service Request to the Office of Technology Services (OTech). The Service Request is located at https://cssweb.dts.ca.gov. For assistance in completing the Service Request, organizations can contact their OTech Account Manager or Customer Service Representative. Exemptions from this standard may be submitted to OCIO by completing the "OCIO EA Compliance Component Template" with an attached "E-Hub Exemption Request" form.

Further information on E-Hub implementation and exemptions requests can be found in the Statewide Information Management Manual (SIMM) under the Enterprise Architecture Standards section located at: http://www.cio.ca.gov/Government/IT_Policy/SIMM.html